McAfee®

virusscan

professional™

Guia do usuário

Versão 9.0

McAfee®

COPYRIGHT

Copyright © 2005 McAfee Inc. Technology, Inc. Todos os direitos reservados. Nenhuma parte desta publicação pode ser reproduzida, transmitida, transcrita, armazenada em um sistema de recuperação ou traduzida para qualquer idioma em qualquer forma ou por qualquer meio sem a permissão, por escrito, da Network Associates Technology, Inc., seus fornecedores ou empresas associadas. Para obter essa permissão, escreva para o departamento jurídico da McAfee do Brasil: R. Verbo Divino, 1227 2o. Andar Chácara Sto Antonio São Paulo - SP 04719-002 Brasil ou ligue para: (55 11) 5180 6610 (55 11) 5180 6686 fax.

ATRIBUIÇÕES DE MARCAS COMERCIAIS

ACTIVE FIREWALL, ACTIVE SECURITY, ACTIVESECURITY (E EM KATAKANA), ACTIVESHIELD, ANTIVIRUS ANYWARE AND DESIGN, CLEAN-UP, DESIGN (E ESTILIZADO), DESIGN (N ESTILIZADO), ENTERCEPT, ENTERPRISE SECURECAST, ENTERPRISE SECURECAST (E EM KATAKANA), EPOLICY ORCHESTRATOR, FIRST AID, FORCEFIELD, GMT, GROUPSHIELD, GROUPSHIELD (E EM KATAKANA), GUARD DOG, HOMEGUARD, HUNTER, INTRUSHIELD, INTRUSION PREVENTION THROUGH INNOVATION, M AND DESIGN, MCAFEE, MCAFEE (E EM KATAKANA), MCAFEE AND DESIGN, MCAFEE.COM, MCAFEE VIRUSSCAN, NA NETWORK ASSOCIATES, NET TOOLS, NET TOOLS (E EM KATAKANA), NETCRYPTO, NETOCTOPUS, NETSCAN, NETSHIELD, NETWORK ASSOCIATES, NETWORK ASSOCIATES COLLISEUM, NETXRAY, NOTESGUARD, NUTS & BOLTS, OIL CHANGE, PC MEDIC, PCNOTARY, PRIMESUPPORT, RINGFENCE, ROUTER PM, SECURECAST, SECURESELECT, SPAMKILLER, STALKER, THREATSCAN, TIS, TMEG, TOTAL VIRUS DEFENSE, TRUSTED MAIL, UNINSTALLER, VIREX, VIRUS FORUM, VIRUSCAN, VIRUSSCAN, VIRUSSCAN (E EM KATAKANA), WEBSCAN, WEBSHIELD, WEBSHIELD (E EM KATAKANA), WEBSTALKER, WEBWALL, WHAT'S THE STATE OF YOUR IDS?, WHO'S WATCHING YOUR NETWORK, YOUR E-BUSINESS DEFENDER, YOUR NETWORK. OUR BUSINESS. são marcas registradas ou marcas comerciais da McAfee, Inc. e/ou de suas empresas associadas nos EUA e/ou outros países. O vermelho em relação à segurança é característica dos produtos da marca McAfee. Todas as outras marcas registradas e não registradas contidas neste documento são de propriedade exclusiva de seus respectivos proprietários.

INFORMAÇÕES SOBRE LICENÇA

Contrato de licença

AVISO A TODOS OS USUÁRIOS: LEIA ATENTAMENTE O CONTRATO LEGAL CORRESPONDENTE À LICENÇA ADQUIRIDA POR VOCÊ. NELE, ESTÃO DEFINIDOS OS TERMOS E AS CONDIÇÕES GERAIS PARA A UTILIZAÇÃO DO SOFTWARE LICENCIADO. CASO NÃO SAIBA O TIPO DE LICENÇA QUE VOCÊ ADQUIRIU, CONSULTE A DOCUMENTAÇÃO RELACIONADA À COMPRA E VENDA OU À CONCESSÃO DE LICENÇA, INCLUÍDA NO PACOTE DO SOFTWARE OU FORNECIDA SEPARADAMENTE (COMO UM LIVRETO, UM ARQUIVO NO CD DO PRODUTO OU UM ARQUIVO DISPONÍVEL NO SITE DO QUAL O PACOTE DE SOFTWARE FOI OBTIDO POR DOWNLOAD). SE VOCÊ NÃO CONCORDAR COM TODOS OS TERMOS ESTABELECIDOS NO CONTRATO, NÃO INSTALE O SOFTWARE. SE APLICÁVEL, VOCÊ PODERÁ DEVOLVER O PRODUTO À MCAFEE, INC. OU AO LOCAL DA AQUISIÇÃO PARA OBTER UM REEMBOLSO TOTAL.

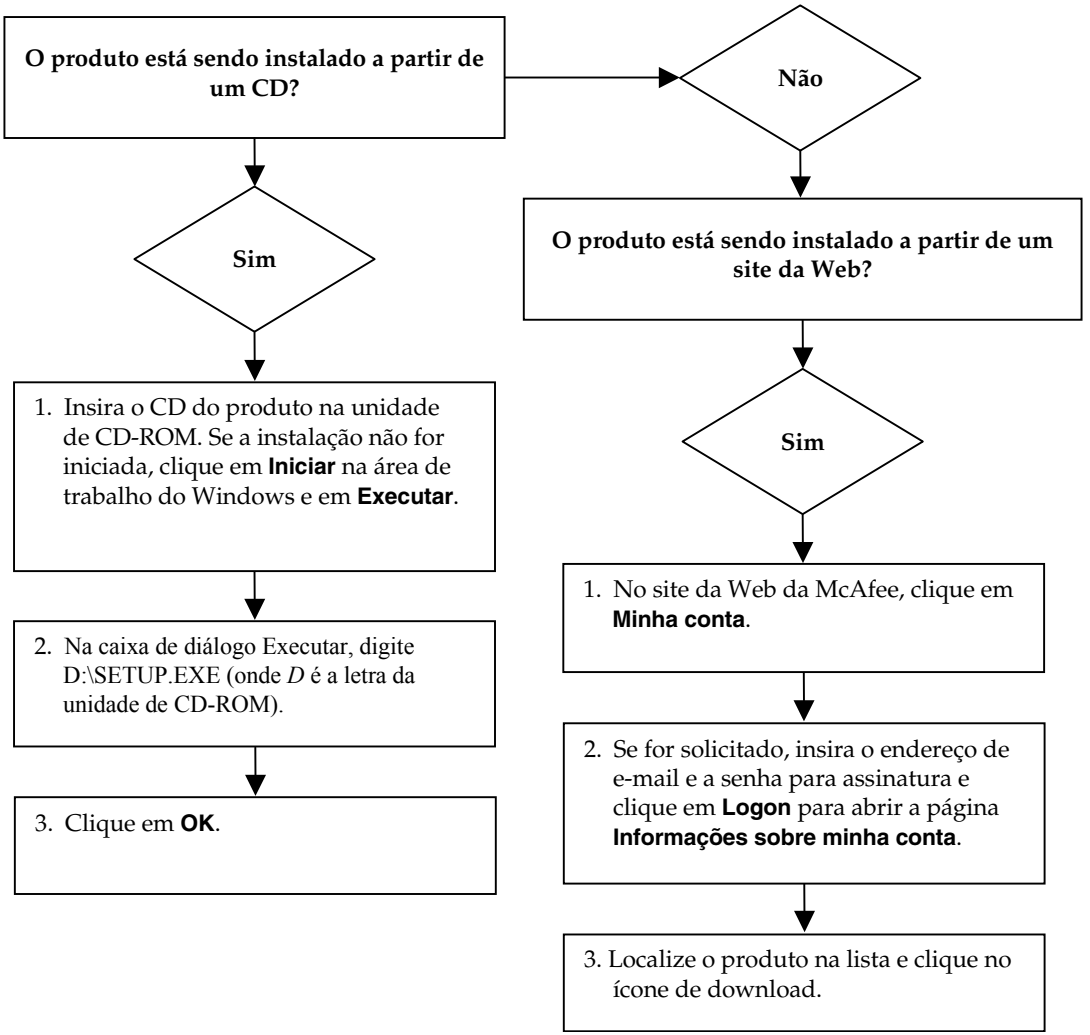
Atribuições

Este produto inclui ou pode incluir:

♦ Software desenvolvido pela OpenSSL Project para uso no OpenSSL Toolkit (http://www.openssl.org/). ♦ Software de criptografia desenvolvido por Eric A. Young e software desenvolvido por Tim J. Hudson. ♦ Alguns softwares que estão licenciados (ou sublicenciados) para o usuário de acordo com o GNU General Public License (GPL) ou com outras licenças de Software Gratuito que, entre outros direitos, permitem que o usuário copie, modifique ou redistribua determinados programas, ou partes deles, e também tenha acesso ao código fonte. O GPL requer que, para qualquer software coberto pelo GPL que seja distribuído para usuários em formato binário executável, o código fonte também seja disponibilizado. Para qualquer um desses softwares cobertos pelo GPL, o código fonte está disponibilizado neste CD. Se uma licença de Software Gratuito exigir que a McAfee, Inc. forneça direitos de uso, cópia ou modificação de um programa de software mais abrangentes que os direitos concedidos neste contrato, eles terão precedência sobre as restrições e os direitos mencionados neste documento. ♦ Software originalmente desenvolvido por Henry Spencer, Copyright 1992, 1993, 1994, 1997 Henry Spencer. ♦ Software originalmente desenvolvido por Robert Nordier, Copyright © 1996-7 Robert Nordier. ♦ Software desenvolvido por Douglas W. Sauder. ♦ Software desenvolvido pela Apache Software Foundation (http://www.apache.org/). Uma cópia do contrato de licença deste software pode ser encontrada em www.apache.org/licenses/LICENSE-2.0.txt. ♦ International Components for Unicode ("ICU") Copyright © 1995-2002 International Business Machines Corporation e outros. ♦ Software desenvolvido pela CrystalClear Software, Inc., Copyright © 2000 CrystalClear Software, Inc. ♦ Tecnologia FEAD® Optimizer®, Copyright Netopsystems AG, Berlim, Alemanha. ♦ Outside In® Viewer Technology © 1992-2001 Stellent Chicago, Inc. e/ou Outside In® HTML Export, © 2001 Stellent Chicago, Inc. ♦ Software de propriedade da Thai Open Source Software Center Ltd. e Clark Cooper, © 1998, 1999, 2000. ♦ Software de propriedade dos mantenedores da Expat. ♦ Software de propriedade de The Regents of the University of California, © 1989. ♦ Software de propriedade de Gunnar Ritter. ♦ Software de propriedade da Sun Microsystems®, Inc.© 2003. ♦ Software de propriedade de Gisle Aas. © 1995-2003. ♦ Software de propriedade de Michael A. Chase, © 1999-2000. ♦ Software de propriedade de Neil Winton, © 1995-1996. ♦ Software de propriedade da RSA Data Security, Inc., © 1990-1992. ♦ Software de propriedade de Sean M. Burke, © 1999, 2000. ♦ Software de propriedade de Martijn Koster, © 1995. ♦ Software de propriedade de Brad Appleton, © 1996-1999. ♦ Software de propriedade de Michael G. Schwern, © 2001. ♦ Software de propriedade de Graham Barr, © 1998. ♦ Software de propriedade de Larry Wall e Clark Cooper, © 1998-2000. ♦ Software de propriedade de Frodo Looijaard, © 1997. ♦ Software de propriedade da Python Software Foundation, Copyright © 2001, 2002, 2003. Uma cópia do contrato de licença deste software pode ser encontrada em www.python.org. ♦ Software de propriedade de Beman Dawes, © 1994-1999, 2002. ♦ Software desenvolvido por Andrew Lumsdaine, Lie-Quan Lee e Jeremy G. Siek © 1997-2000 University of Notre Dame. ♦ Software de propriedade de Simone Bordet & Marco Cravero, © 2002. ♦ Software de propriedade de Stephen Purcell, © 2001. ♦ Software desenvolvido por Indiana University Extreme! Lab (http://www.extreme.indiana.edu/). ♦ Software de propriedade da International Business Machines Corporation e outros, © 1995-2003. ♦ Software desenvolvido pela University of California, Berkeley e seus contribuintes. ♦ Software desenvolvido por Ralf S. Engelschall <rse@engelschall.com> para uso no projeto mod_ssl (http://www.modssl.org/). ♦ Software de propriedade de Kevlin Henney, © 2000-2002. ♦ Software de propriedade de Peter Dimov e Multi Media Ltd. © 2001, 2002. ♦ Software de propriedade de David Abrahams, © 2001, 2002. Consulte http://www.boost.org/libs/bind/bind.html para obter a documentação. ♦ Software de propriedade de Steve Cleary, Beman Dawes, Howard Hinnant e John Maddock, © 2000. ♦ Software de propriedade da Boost.org, © 1999-2002. ♦ Software de propriedade de Nicolai M. Josuttis, © 1999. ♦ Software de propriedade de Jeremy Siek, © 1999-2001. ♦ Software de propriedade de Daryle Walker, © 2001. ♦ Software de propriedade de Chuck Allison e Jeremy Siek, © 2001, 2002. ♦ Software de propriedade de Samuel Krempp, © 2001. Consulte http://www.boost.org para obter atualizações, documentação e histórico de revisão. ♦ Software de propriedade de Doug Gregor (gregod@cs.rpi.edu), © 2001, 2002. ♦ Software de propriedade de Cadenza New Zealand Ltd., © 2000. ♦ Software de propriedade de Jens Maurer, © 2000, 2001. ♦ Software de propriedade de Jaakko Järvi (jaakko.jarvi@cs.utu.fi), © 1999, 2000. ♦ Software de propriedade de Ronald Garcia, © 2002. ♦ Software de propriedade de David Abrahams, Jeremy Siek e Daryle Walker, © 1999-2001. ♦ Software de propriedade de Stephen Cleary (shammah@voyager.net), © 2000. ♦ Software de propriedade de Housemarque Oy <http://www.housemarque.com>, © 2001. ♦ Software de propriedade de Paul Moore, © 1999. ♦ Software de propriedade de Dr. John Maddock, © 1998-2002. ♦ Software de propriedade de Greg Colvin e Beman Dawes, © 1998, 1999. ♦ Software de propriedade de Peter Dimov, © 2001, 2002. ♦ Software de propriedade de Jeremy Siek e John R. Bandela, © 2001. ♦ Software de propriedade de Joerg Walter e Mathias Koch, © 2000-2002.

Quick Start Card

Se você estiver instalando o produto a partir de um CD ou do site da Web, imprima esta página de referência para sua conveniência.


O produto está sendo instalado a partir de um CD?
Não
Sim
O produto está sendo instalado a partir de um site da Web?
Sim
1. Insira o CD do produto na unidade de CD-ROM. Se a instalação não for iniciada, clique em **Iniciar** na área de trabalho do Windows e em **Executar**.
2. Na caixa de diálogo Executar, digite D:\SETUP.EXE (onde *D* é a letra da unidade de CD-ROM).
3. Clique em **OK**.
1. No site da Web da McAfee, clique em **Minha conta**.
2. Se for solicitado, insira o endereço de e-mail e a senha para assinatura e clique em **Logon** para abrir a página **Informações sobre minha conta**.
3. Localize o produto na lista e clique no ícone de download.

A McAfee reserva-se o direito de alterar as diretivas e os planos de atualização e suporte a qualquer momento, sem aviso prévio. McAfee e VirusScan são marcas registradas da McAfee, Inc. e/ou de suas empresas afiliadas nos EUA e/ou em outros países.
© 2005 Networks Associates Technology, Inc. Todos os direitos reservados.

Para obter mais informações

Para exibir os Guias de usuário no CD do produto, verifique se você tem o Acrobat Reader instalado. Se não tiver, instale-o a partir do CD do produto McAfee.

1. Insira o CD do produto na unidade de CD-ROM.
2. Abra o Windows Explorer: clique em **Iniciar** na área de trabalho do Windows e, em seguida, clique em **Pesquisar**.
3. Localize a pasta de manuais e clique duas vezes no .PDF do Guia do usuário que deseja abrir.

Benefícios do registro

Recomendamos que você siga as etapas do produto para transmitir o registro diretamente para nós. O registro assegura que você receberá assistência técnica imediata de pessoas experientes, além dos seguintes benefícios:

- Suporte eletrônico GRATUITO
- Atualizações de arquivo de definição de vírus (.DAT) durante um ano a partir da instalação, após a compra do software VirusScan.

  Vá para http://br.mcafee.com/ para obter os preços referentes a mais um ano de assinaturas de vírus.
- 30 dias de garantia, que assegura a substituição do CD do software caso ele esteja com defeito ou danificado.
- Atualizações de filtro do SpamKiller por um ano a partir da instalação, após a compra do software SpamKiller.

  Vá para http://br.mcafee.com/para obter os preços referentes a mais um ano de atualizações de filtro.
- Atualizações do McAfee Internet Security Suite durante um ano a partir da instalação, após a compra do software MIS.

  Vá para http://br.mcafee.com/ para obter os preços referentes a mais um ano de atualizações de conteúdo.

Suporte técnico

Para obter suporte técnico, visite http://www.mcafeeajuda.com/. Nosso site de suporte oferece 24 horas de acesso ao Assistente de respostas de fácil utilização, para que você possa obter soluções para as perguntas de suporte mais comuns.

Os usuários experientes também podem tentar nossas opções avançadas, que incluem uma pesquisa de palavra-chave e nossa árvore de ajuda. Se você não encontrar uma solução para o seu problema, ainda poderá acessar as opções GRATUITAS Chat Now! e E-mail Express! O bate-papo e o e-mail ajudarão você a entrar em contato com nossos engenheiros de suporte qualificados pela Internet, de forma rápida e gratuita. Você também pode obter informações sobre o suporte telefônico em http://www.mcafeeajuda.com/.

Números de telefone para emergências

País	Números de telefone
África do Sul	011 700-8216
Alemanha	06 966 404 330
Áustria	017 908 75 810
Bélgica	02 27 50 703
Brasil	55 11 4196 7077
Dinamarca	03 5258 321
Espanha	901-120 175 (* tarifado)
Finlândia	09 229 06 000
França	01 70 20 0 008
Holanda	020 504 0586
Irlanda	01 601 55 80
Itália	02 45 28 15 10
Luxemburgo	040 666 15670
Noruega	02 3050420
Portugal	00 31 20 586 6430 (em inglês)
Reino Unido	020 794 901 07
Suécia	08 57 92 9004
Suíça	022 310 1033

Conteúdo

Quick Start Card . . . . . **iii**

1 Introdução **9**

Novos recursos 9
Requisitos do sistema 11
Testando o VirusScan 11
Testando o ActiveShield 11
Testando o recurso Fazer varredura 12
Usando o McAfee SecurityCenter 14

2 Usando o McAfee VirusScan **15**

Usando o ActiveShield 15
Ativando ou desativando o ActiveShield 15
Configurando opções do ActiveShield 16
Se o ActiveShield localizar um vírus 25
Fazendo a varredura manual do computador 28
Fazendo a varredura manual para vírus e programas potencialmente indesejados 28
Fazendo a varredura automática para vírus e programas potencialmente indesejados 33
Se a opção Fazer varredura encontrar um vírus ou programa potencialmente indesejado 35
Gerenciando arquivos em quarentena 36

3 Usando o software Professional Edition **39**

Usando o McAfee SpamKiller 39
Visão geral 39
Trabalhando com mensagens bloqueadas e aceitas 41

Usando o McAfee Shredder 48
Por que o Windows deixa alguns vestígios do arquivo? 48
O que o McAfee Shredder apaga? 48
Apagando arquivos permanentemente no Windows Explorer 48
Esvaziando a Lixeira do Windows 49
Personalizando as configurações do Shredder 49

Índice 51

Introdução 1

Bem-vindo ao McAfee VirusScan. O McAfee VirusScan Professional Edition contém o McAfee VirusScan, o McAfee SpamKiller e o McAfee Shredder. Consulte *Usando o software Professional Edition* na página 39 para obter mais informações sobre esses programas adicionais.

> **OBSERVAÇÃO**
> Esta é apenas uma visão geral. Para obter informações detalhadas, consulte a Ajuda on-line do VirusScan, SpamKiller ou Shredder.

O McAfee VirusScan é um serviço de assinatura antivírus que oferece uma proteção contra vírus abrangente, confiável e atualizada. Controlado pela tecnologia de varredura premiada da McAfee, o VirusScan protege o seu computador contra vírus, worms, Cavalos de Tróia, scripts mal-intencionados e ataques híbridos.

Com ele, você irá aproveitar os seguintes recursos:

ActiveShield — Faz a varredura dos arquivos quando eles são acessados por você ou por seu computador.

Fazer varredura — Procura vírus e programas potencialmente indesejados em unidades de disco rígido, em disquetes e em arquivos e pastas individuais.

Quarentena — Criptografa e isola temporariamente arquivos infectados e suspeitos na pasta de quarentena até que uma ação apropriada possa ser executada.

Detecção de atividade hostil — Monitora o computador em relação a atividades de vírus causadas por scripts mal-intencionados e atividades de worm.

Novos recursos

Esta versão do VirusScan possui os seguintes novos recursos:

- **Fazer a varredura de programas indesejados**
  O VirusScan pode fazer a varredura de programas indesejados (incluindo spyware, adware e discadores) durante a varredura manual, varredura de e-mails enviados, mensagens instantâneas (MI) através do menu de atalho do Windows Explorer e do ícone do Microsoft Outlook localizado na barra de ferramentas.

- **Fazer a varredura de grandes anexos enviados**
  Para lidar com o maior número de conexões de banda larga à Internet e provedores de serviços que aumentam os tamanhos de transmissão e armazenamento de e-mails, o VirusScan foi otimizado para fazer a varredura de anexos de e-mail grandes sem interferir nos valores de tempo limite do programa de e-mail.

- **Varredura de e-mails**
  O VirusScan faz a varredura automática de e-mails e anexos de e-mail recebidos (POP3) e enviados (SMTP) dos clientes de e-mail mais populares, incluindo o Microsoft Outlook, Netscape Mail, Eudora e Pegasus.

- **Varredura de mensagem instantânea**
  O VirusScan faz a varredura automática dos arquivos recebidos dos clientes de mensagens instantâneas mais populares, incluindo o Yahoo Messenger, AOL Instant Messenger e MSN Messenger.

- **Detecção de atividade hostil**
  O VirusScan fornece o ScriptStopper™ e o WormStopper™ para detectar, alertar e bloquear atividades de vírus causadas por scripts mal-intencionados e atividades de worm.

- **Limpeza automática da infecção de arquivos**
  O VirusScan tenta limpar automaticamente os arquivos infectados ou suspeitos assim que são detectados.

- **Varredura programada**
  Agora você pode programar uma varredura automática em intervalos especificados para procurar vírus em todo o computador.

- **Quarentena de arquivos**
  É possível usar o recurso Quarentena para criptografar e isolar temporariamente arquivos infectados e suspeitos na pasta de quarentena até que uma ação apropriada possa ser executada. Depois de limpo, um arquivo em quarentena pode ser restaurado para o local original.

- **Enviar arquivos para a AVERT**
  Agora, o VirusScan envia os arquivos suspeitos diretamente do recurso Quarentena para a McAfee AntiVirus Emergency Response Team (AVERT™) para fins de pesquisa.

- **Relatório do Virus Map**
  Agora você pode enviar de forma anônima informações de rastreamento de vírus para serem incluídas no World Virus Map. Você pode registrar-se automaticamente neste recurso gratuito e seguro e exibir as taxas de infecção mundiais mais recentes através do McAfee SecurityCenter.

Requisitos do sistema

- Microsoft® Windows 98, Me, 2000 ou XP
- Computador pessoal com processador
  Windows 98 ou Me: Pentium 150 MHz ou superior
  Windows 2000 ou XP: Pentium de 233 MHz ou superior
- RAM
  Windows 98: 32 MB (64 MB recomendado)
  Windows Me, 2000 ou XP: 64 MB (128 MB recomendado)
- 40 MB de espaço em disco rígido
- Microsoft® Internet Explorer 5.5 ou posterior

OBSERVAÇÃO
Para atualizar para a versão mais recente do Internet Explorer, visite o site da Microsoft em http://www.microsoft.com/brasil/.

Testando o VirusScan

Antes de começar a usar o VirusScan, recomenda-se testar a instalação. Execute as etapas a seguir para testar separadamente os recursos Fazer varredura e ActiveShield.

Testando o ActiveShield

Para testar o ActiveShield:

1. Vá para http://www.eicar.com/ no navegador da Web.
2. Clique no link **The AntiVirus testfile eicar.com**.
3. Deslize até o final da página. Em **Download**, você verá quatro links.
4. Clique em **eicar.com**.

Se o ActiveShield estiver funcionando adequadamente, ele detectará o arquivo eicar.com imediatamente depois que você clicar no link. Você pode tentar excluir os arquivos infectados ou colocá-los em quarentena para saber como o ActiveShield lidará com o vírus. Consulte *Se o ActiveShield localizar um vírus* na página 25 para obter detalhes.

Testando o recurso Fazer varredura

Para testar o recurso Fazer varredura, desative o ActiveShield para evitar que ele detecte os arquivos infectados antes do Fazer varredura e, depois, faça o download dos arquivos de teste.

Para fazer o download dos arquivos de teste:

1. Desative o ActiveShield: Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Desativar**.
2. Faça o download dos arquivos de teste EICAR no site da EICAR:
   a. Vá para http://www.eicar.com/.
   b. Clique no link **The AntiVirus testfile eicar.com**.
   c. Deslize até o final da página. Em **Fazer o download**, você verá os seguintes links:

      eicar.com contém uma linha de texto que o VirusScan detectará como vírus.

      eicar.com.txt (opcional) é o mesmo arquivo, mas com outro nome, para os usuários que não conseguirem fazer o download pelo primeiro link. Simplesmente renomeie o arquivo "eicar.com" após o download.

      eicar_com.zip é uma cópia do vírus de teste dentro de um arquivo compactado .ZIP (um arquivo WinZip™).

      eicarcom2.zip é uma cópia do vírus de teste dentro de um arquivo compactado .ZIP, que está armazenado dentro de um arquivo compactado .ZIP.

   d. Clique em cada link para fazer o download dos arquivos correspondentes. Em cada link, será exibida a caixa de diálogo **Download de arquivo**.
   e. Clique em **Salvar**, clique no botão **Criar nova pasta** e renomeie a **Pasta de varredura do VSO**.
   f. Clique duas vezes em **Pasta de varredura do VSO** e clique em **Salvar** novamente em cada caixa de diálogo **Salvar como**.
3. Quando terminar de fazer o download dos arquivos, feche o Internet Explorer.
4. Ative o ActiveShield: Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Ativar**.

Para testar o recurso Fazer varredura:

1. Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Fazer varredura**.
2. Usando a árvore de diretório no painel esquerdo da caixa de diálogo, vá para **Pasta de varredura do VSO** onde os arquivos foram salvos:
   a. Clique no sinal de adição (**+**) ao lado do ícone da unidade C.
   b. Clique em **Pasta de varredura do VSO** para destacá-la (não clique no sinal de adição (**+**) que aparece ao lado dessa opção).

      Isso instruirá o recurso Fazer varredura a procurar vírus somente nessa pasta. Você também pode colocar os arquivos em locais aleatórios na unidade de disco rígido para fazer uma demonstração mais convincente das habilidades do recurso de varredura.
3. Na área **Opções de varredura** da caixa de diálogo **Fazer varredura**, certifique-se de que todas as opções estejam selecionadas.
4. Clique em **Fazer varredura** no canto inferior direito da caixa de diálogo.

   O VirusScan faz a varredura da **Pasta de varredura do VSO**. Os arquivos de teste EICAR que você salvou nessa pasta serão exibidos em **Lista de arquivos detectados**. Isso significa que a varredura está funcionando adequadamente.

Tente excluir os arquivos infectados ou colocá-los em quarentena para saber como o recurso Fazer varredura lidará com os vírus. Consulte *Se a opção Fazer varredura encontrar um vírus ou programa potencialmente indesejado* na página 35 para obter detalhes.

Usando o McAfee SecurityCenter

O McAfee SecurityCenter é a sua loja de segurança, acessível através de um ícone fornecido na bandeja de sistema do Windows ou na área de trabalho do Windows. Ele permite executar as seguintes tarefas:

- Obter uma análise de segurança gratuita do computador.
- Iniciar, gerenciar e configurar todas as assinaturas do McAfee a partir de um ícone.
- Ver os alertas de vírus atualizados continuamente e as informações mais recentes sobre produtos.
- Obter links rápidos para perguntas freqüentes e detalhes de conta no site da McAfee.

> **OBSERVAÇÃO**
> Para obter mais informações sobre esses recursos, clique em **Ajuda** na caixa de diálogo **SecurityCenter**.

Enquanto o SecurityCenter estiver em execução e todos os recursos do McAfee instalados no computador estiverem ativados, um ícone M vermelho será exibido na bandeja de sistema do Windows. Essa área fica normalmente no canto inferior direito da área de trabalho do Windows e contém o relógio.

Se um ou mais aplicativos do McAfee instalados no computador estiverem desativados, o ícone da McAfee ficará preto .

Para abrir o McAfee SecurityCenter:

1. Clique com o botão direito do mouse no ícone da McAfee .
2. Clique em **Abrir o Security Center**.

Para acessar um recurso do VirusScan:

1. Clique com o botão direito do mouse no ícone da McAfee .
2. Aponte para **VirusScan** e clique no recurso a ser usado.

Usando o McAfee VirusScan 2

Usando o ActiveShield

Quando o ActiveShield for iniciado (carregado na memória do computador) e ativado, ele estará protegendo constantemente o computador. O ActiveShield faz a varredura dos arquivos quando eles são acessados por você ou por seu computador. Ao detectar um arquivo infectado, ele automaticamente tenta limpar o vírus. Se ele não conseguir limpar o vírus, você poderá colocar o arquivo em quarentena ou excluí-lo.

Ativando ou desativando o ActiveShield

Por padrão, o ActiveShield é iniciado (carregado na memória do computador) e ativado (representado por um ícone vermelho na bandeja de sistema do Windows) assim que você reinicia o computador após o processo de instalação.

Se o ActiveShield for interrompido (não carregado) ou desativado (representado por um ícone preto), você poderá executá-lo manualmente, bem como configurá-lo para que seja iniciado automaticamente quando o Windows for iniciado.

Ativando o ActiveShield

Para ativar o ActiveShield somente nesta sessão do Windows:

Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Ativar**. O ícone da McAfee é alterado para um vermelho.

Se o ActiveShield ainda estiver configurado para ser iniciado junto com o Windows, uma mensagem informará que você está protegido contra vírus. Caso contrário, uma caixa de diálogo será exibida, na qual você poderá configurar o ActiveShield para ser iniciado junto com o Windows (Figura 2-1 na página 16).

Desativando o ActiveShield

Para desativar o ActiveShield somente nesta sessão do Windows:

1. Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Desativar**.
2. Clique em **Sim** para confirmar.

   O ícone da McAfee é alterado para um preto.

Se o ActiveShield ainda estiver configurado para ser iniciado junto com o Windows, o computador estará protegido contra vírus novamente quando você reiniciá-lo.

Configurando opções do ActiveShield

Você pode modificar as opções de inicialização e varredura do ActiveShield na guia **ActiveShield** da caixa de diálogo **Opções do VirusScan** (Figura 2-1), que pode ser acessada através do ícone da McAfee na bandeja de sistema do Windows.

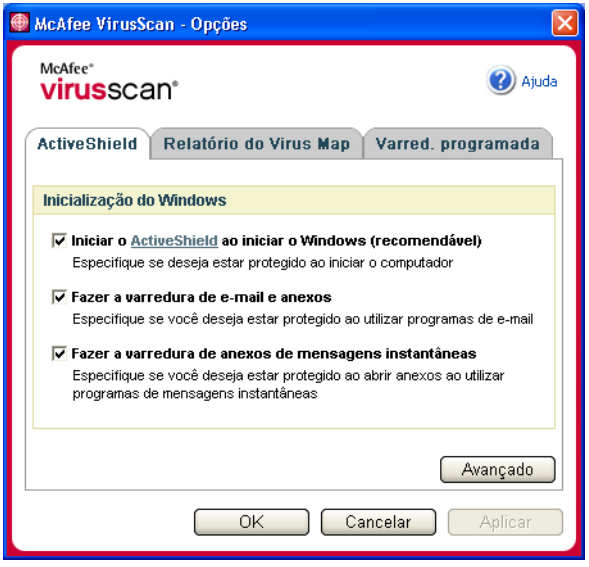

McAfee VirusScan - Opções
McAfee
virusscan
Ajuda
ActiveShield
Relatório do Vírus Map
Varred. programada
Inicialização do Windows
Iniciar o ActiveShield ao iniciar o Windows (recomendável)
Especifique se deseja estar protegido ao iniciar o computador
Fazer a varredura de e-mail e anexos
Especifique se você deseja estar protegido ao utilizar programas de e-mail
Fazer a varredura de anexos de mensagens instantâneas
Especifique se você deseja estar protegido ao abrir anexos ao utilizar programas de mensagens instantâneas
Avançado
OK
Cancelar
Aplicar

Figura 2-1. Opções do ActiveShield

Iniciando o ActiveShield

Por padrão, o ActiveShield é iniciado (carregado na memória do computador) e ativado (representado por um vermelho) assim que você reinicia o computador após o processo de instalação.

Se o ActiveShield for interrompido (representado por um preto), você poderá configurá-lo para que seja iniciado automaticamente junto com o Windows (recomendável).

> **OBSERVAÇÃO**
> Durante a atualização para VirusScan, o **Assistente de atualização** pode fechar o ActiveShield temporariamente para instalar novos arquivos. Quando o **Assistente de atualização** solicitar que você clique em **Concluir**, o ActiveShield será iniciado novamente.

Para iniciar o ActiveShield automaticamente junto com o Windows:

1. Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Opções**.

   A caixa de diálogo **Opções do VirusScan** será aberta (Figura 2-1 na página 16).

2. Marque a caixa de seleção **Iniciar o ActiveShield quando o Windows for iniciado (recomendável)** e clique em **Aplicar** para salvar as alterações.

3. Clique em **OK** para confirmar e, em seguida, clique em **OK** novamente.

Interrompendo o ActiveShield

> **AVISO**
> Se você interromper o ActiveShield, o computador não estará protegido contra vírus. Se for necessário interromper o ActiveShield, certifique-se de que não esteja conectado à Internet, a não ser que seja para atualizar o VirusScan.

Para que o ActiveShield não seja iniciado junto com o Windows:

1. Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Opções**.

   A caixa de diálogo **Opções do VirusScan** será aberta (Figura 2-1 na página 16).

2. Desmarque a caixa **Iniciar o ActiveShield quando o Windows for iniciado (recomendável)** e clique em **Aplicar** para salvar as alterações.

3. Clique em **OK** para confirmar e, em seguida, clique em **OK** novamente.

Fazendo a varredura de e-mails e anexos

Por padrão, a varredura de e-mail e a limpeza automática são ativadas através das opções **Fazer a varredura de e-mail e anexos** (Figura 2-1 na página 16) e **Limpar automaticamente anexos infectados (recomendável)** (Figura 2-2 na página 20).

Quando essas duas opções estão ativadas, o ActiveShield faz a varredura automaticamente e tenta limpar as mensagens e os anexos de e-mail infectados enviados (SMTP) e recebidos (POP3) pelos clientes de e-mail mais populares:

- Microsoft Outlook Express 4.0 ou posterior
- Microsoft Outlook 97 ou posterior
- Netscape Messenger 4.0 ou posterior
- Netscape Mail 6.0 ou posterior
- Eudora Light 3.0 ou posterior
- Eudora Pro 4.0 ou posterior
- Eudora 5.0 ou posterior
- Pegasus 4.0 ou posterior

OBSERVAÇÃO

A varredura de e-mail não é suportada nos seguintes clientes de e-mail: clientes baseados na Web, IMAP, AOL, POP3 SSL e Lotus Notes. No entanto, o ActiveShield faz a varredura de anexos de e-mail quando eles são abertos.

Se você desativar a opção **Fazer a varredura de e-mail e anexos**, as opções de Varredura de e-mail (Figura 2-2 na página 20) e de WormStopper (Figura 2-5 na página 25) serão desativadas automaticamente. Se você desativar a varredura de e-mails enviados, as opções do WormStopper serão automaticamente desativadas.

Se você alterar as opções de varredura de e-mails, reinicie seu programa de e-mail para efetuar essas alterações.

E-mails recebidos

Se uma mensagem ou um anexo de e-mail recebido estiver infectado, o ActiveShield executará as seguintes etapas:

- Tentará limpar o e-mail infectado.
- Tentará colocar em quarentena ou excluir o e-mail que não pôde ser limpo.
- Incluirá um arquivo de alerta no e-mail recebido; esse arquivo conterá informações sobre as ações que devem ser executadas para remover a infecção.

E-mails enviados

Se uma mensagem ou um anexo de e-mail enviado estiver infectado, o ActiveShield executará as seguintes etapas:

- Tentará limpar o e-mail infectado.
- Tentará colocar em quarentena ou excluir o e-mail que não pôde ser limpo.
- Enviará um arquivo de alerta para você em um novo e-mail; esse arquivo conterá informações sobre as ações que devem ser executadas para remover a infecção.

> **OBSERVAÇÃO**
> Para obter detalhes sobre erros de varredura de e-mails enviados, consulte a Ajuda on-line.

Por padrão, o ActiveShield faz a varredura de e-mails recebidos e enviados. No entanto, para um melhor controle, você pode configurar o ActiveShield para fazer a varredura somente de e-mails recebidos ou enviados.

Para desativar a varredura de e-mails recebidos ou enviados:

1. Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Opções**.
2. Clique em **Avançado** e, em seguida, clique na guia **Varredura de e-mail** (Figura 2-2 na página 20).
3. Desmarque **Mensagens de e-mail recebidas** ou **Mensagens de e-mail enviadas** e clique em **OK**.

Se o servidor de e-mail estiver definido somente para enviar e receber e-mails quando você estiver no computador, opte por desativar a limpeza automática, a fim de que os alertas o lembrem de limpar os e-mails infectados. Siga as etapas abaixo para desativar a limpeza automática e consulte *Gerenciando e-mails infectados* na página 26 para obter detalhes sobre como responder aos alertas.

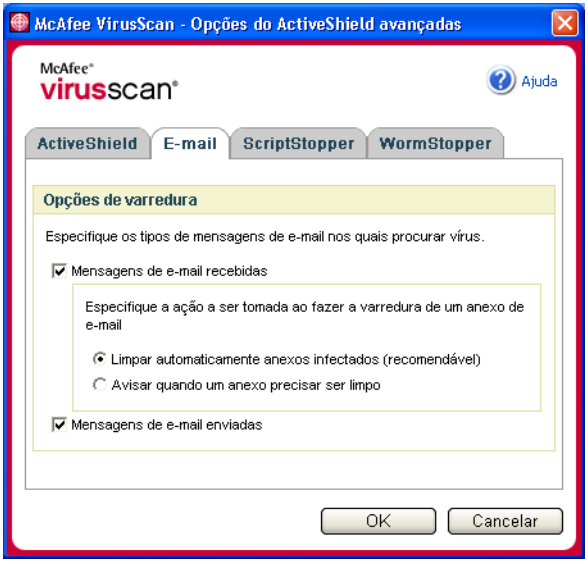


Figura 2-2. Opções de Varredura de e-mail

Para desativar a limpeza automática dos e-mails infectados:

1. Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Opções**.
2. Clique em **Avançado** e, em seguida, clique na guia **Varredura de e-mail** (Figura 2-2).
3. Clique em **Avisar quando um anexo precisar ser limpo** e, depois, clique em **OK**.

Fazendo a varredura de anexos de mensagens instantâneas recebidas

Por padrão, a varredura de anexos de mensagens instantâneas é ativada através da opção **Fazer a varredura de anexos de mensagens instantâneas** (Figura 2-1 na página 16).

Quando esta opção é ativada, o VirusScan faz a varredura automaticamente e tenta limpar os anexos de mensagens instantâneas infectadas recebidas pelos clientes de mensagem instantânea mais populares:

- MSN Messenger 6.0 ou posterior
- Yahoo Messenger 4.1 ou posterior
- AOL Instant Messenger 2.1 ou posterior

OBSERVAÇÃO
Para sua proteção, não será possível desativar a limpeza automática dos anexos de mensagens instantâneas.

Se um anexo de mensagem instantânea recebida estiver infectado, o VirusScan executará as seguintes etapas:

- Tentará limpar a mensagem infectada.
- Solicitará que você coloque em quarentena ou exclua uma mensagem que não pôde ser limpa.

Fazendo a varredura de todos os arquivos

Se você definir o ActiveShield para usar a opção padrão **Todos os arquivos (recomendável)**, ele fará a varredura de todos os tipos de arquivo usados pelo computador à medida que o computador tentar utilizá-los. Use esta opção para obter a varredura mais completa possível.

Para definir o ActiveShield para fazer a varredura de todos os tipos de arquivo:

1. Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Opções**.
2. Clique em **Avançado** e, depois, clique na guia **ActiveShield** (Figura 2-3 na página 22).
3. Clique em **Todos os arquivos (recomendável)** e, depois, clique em **OK**.

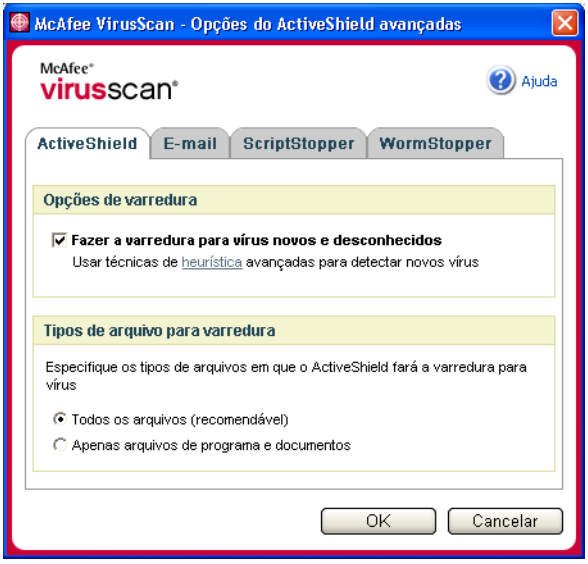


Figura 2-3. Opções avançadas do ActiveShield

Fazendo a varredura somente de arquivos de programa e documentos

Se você definir o ActiveShield para usar a opção **Apenas arquivos de programa e documentos**, ele fará a varredura somente dos arquivos de programa e dos documentos, isentando qualquer outro arquivo usado pelo computador.
O arquivo de assinatura de vírus mais recente (arquivo DAT) determina em quais tipos de arquivo o ActiveShield fará a varredura. Para definir o ActiveShield para fazer a varredura apenas dos arquivos de programa e documentos:

1. Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Opções**.
2. Clique em **Avançado** e, depois, clique na guia **ActiveShield** (Figura 2-3).
3. Clique em **Apenas arquivos de programa e documentos** e, depois, clique em **OK**.

Fazendo a varredura para vírus novos e desconhecidos

Se você definir o ActiveShield para usar a opção padrão **Fazer varredura para vírus novos e desconhecidos (recomendável)**, ele usará técnicas heurísticas avançadas que tentam fazer a correspondência dos arquivos com as assinaturas de vírus conhecidos e, ao mesmo tempo, procurará indícios de vírus desconhecidos nos arquivos.

Para definir o ActiveShield para fazer a varredura em busca de vírus novos e desconhecidos:

1 Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Opções**.

2 Clique em **Avançado** e, depois, clique na guia **ActiveShield** (Figura 2-3 na página 22).

3 Clique em **Fazer varredura para vírus novos e desconhecidos (recomendável)** e, depois, clique em **OK**.

Fazendo a varredura para scripts e worms

O VirusScan monitora o computador em busca de atividades suspeitas que possam representar uma ameaça. Enquanto o VirusScan limpa os vírus, o ScriptStopper™ e o WormStopper™ impedem que vírus, worms e Cavalos de Tróia se espalhem ainda mais.

Os mecanismos de proteção do ScriptStopper e do WormStopper detectam, alertam e bloqueiam atividades mal-intencionadas. As atividades suspeitas podem executar as seguintes ações no computador:

- Uma execução de script que resulta na criação, cópia ou exclusão de arquivos ou na abertura do Registro do Windows.
- Uma tentativa de encaminhar um e-mail para muitas pessoas da lista de endereços.
- Tentativas de encaminhar várias mensagens de e-mail em uma rápida sucessão.

Se você definir o ActiveShield para usar as opções padrão **Ativar ScriptStopper (recomendável)** e **Ativar WormStopper (recomendável)** na caixa de diálogo **Opções avançadas**, o ScriptStopper e o WormStopper monitorarão a execução de scripts e as atividades de e-mail em busca de padrões suspeitos e enviarão um alerta quando um determinado número de e-mails ou destinatários for ultrapassado em um intervalo especificado.

Para definir o ActiveShield para fazer a varredura de scripts mal-intencionados e atividades de worm:

1 Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Opções**.

2 Clique em **Avançado** e, depois, clique na guia **ScriptStopper**.

3 Clique em **Ativar ScriptStopper (recomendável)** (Figura 2-4 na página 24).

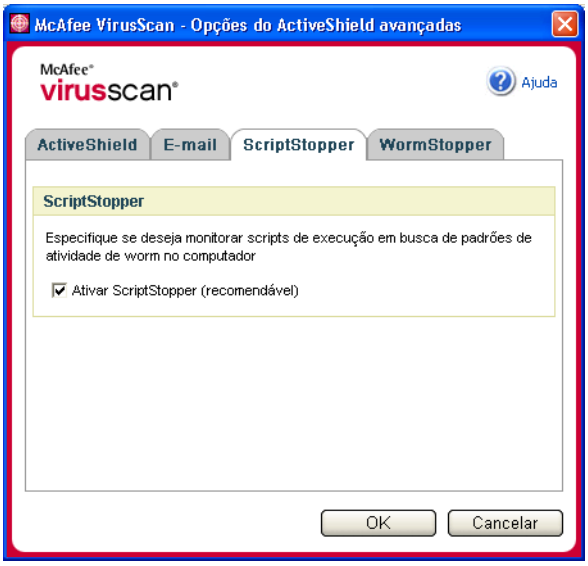


Figura 2-4. Opções do ScriptStopper

4 Clique na guia **WormStopper**, clique em **Ativar WormStopper (recomendável)** e, em seguida, clique em **OK** (Figura 2-5 na página 25).

Por padrão, as seguintes opções detalhadas aparecem ativadas:

- Correspondência de padrão para detectar atividades suspeitas
- Enviar alerta quando um e-mail for enviado para 40 ou mais destinatários
- Enviar alerta quando 5 ou mais e-mails forem enviados dentro de 30 segundos

OBSERVAÇÃO
Se você modificar o número de destinatários ou segundos para monitorar e-mails enviados, isso pode resultar em detecções inválidas. A McAfee recomenda que você clique em **Não** para manter a configuração padrão. Caso contrário, clique em **Sim** para substituir as configurações padrão por suas configurações.

Esta opção pode ser ativada automaticamente depois que um possível worm for detectado pela primeira vez (consulte *Gerenciando possíveis worms* na página 27 para obter detalhes):

- Bloqueio automático de e-mails enviados suspeitos

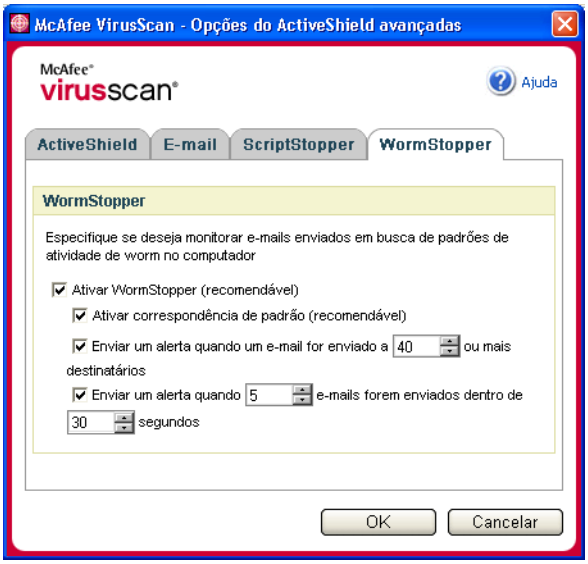

McAfee VirusScan - Opções do ActiveShield avançadas
McAfee
virusscan
Ajuda
ActiveShield
E-mail
ScriptStopper
WormStopper
WormStopper
Especifique se deseja monitorar e-mails enviados em busca de padrões de atividade de worm no computador
Ativar WormStopper (recomendável)
Ativar correspondência de padrão (recomendável)
Enviar um alerta quando um e-mail for enviado a 40 ou mais destinatários
Enviar um alerta quando 5 e-mails forem enviados dentro de 30 segundos
OK
Cancelar

Figura 2-5. Opções do WormStopper

Se o ActiveShield localizar um vírus

Se o ActiveShield localizar um vírus, um alerta de vírus similar à Figura 2-6 será exibido. Na maioria dos vírus, Cavalos de Tróia e worms, o ActiveShield tenta limpar automaticamente o arquivo. Em seguida, você poderá escolher como gerenciar os arquivos infectados, os e-mail infectados, os scripts suspeitos e os possíveis worms, além de especificar se deseja enviar arquivos infectados aos laboratórios AVERT da McAfee para que sejam pesquisados.

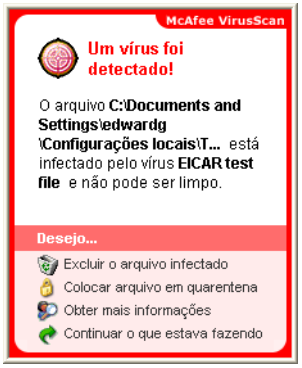

McAfee VirusScan
Um vírus foi detectado!
O arquivo C:\Documents and Settings\edwardg \Configurações locais\T... está infectado pelo vírus EICAR test file e não pode ser limpo.
Desejo...
Excluir o arquivo infectado
Colocar arquivo em quarentena
Obter mais informações
Continuar o que estava fazendo

Figura 2-6. Alerta de vírus

Gerenciando arquivos infectados

1 Se o ActiveShield conseguir limpar o arquivo, você poderá obter mais informações ou ignorar o alerta:

- Clique em **Obter mais informações** para exibir o nome, local e nome de vírus associado ao arquivo infectado.
- Clique em **Continuar o que eu estava fazendo** para ignorar o alerta e fechá-lo.

2 Se o ActiveShield não conseguir limpar o arquivo, clique em **Colocar arquivo em quarentena** para criptografar e isolar temporariamente arquivos infectados e suspeitos no diretório de quarentena até que uma ação apropriada possa ser executada.

Uma mensagem de confirmação é exibida e solicita que você verifique se há vírus em seu computador. Clique em **Fazer varredura** para concluir o processo de quarentena.

3 Se o ActiveShield não puder colocar o arquivo em quarentena, clique em **Excluir o arquivo infectado** para tentar removê-lo.

Gerenciando e-mails infectados

1 Se você desativou a limpeza automática de e-mails, poderá obter mais informações e limpar o e-mail:

a Clique em **Obter mais informações** para exibir o nome do arquivo, o nome do vírus, o status da infecção, o remetente e qualquer assunto associado ao e-mail infectado.

b Clique em **Limpar os anexos infectados**.

2 Se o ActiveShield não conseguir limpar o e-mail, clique em **Colocar os anexos em quarentena** para criptografar e isolar temporariamente os arquivos infectados e suspeitos no diretório de quarentena até que uma ação apropriada possa ser executada.

Uma mensagem de confirmação é exibida e solicita que você verifique se há vírus em seu computador. Clique em **Fazer varredura** para concluir o processo de quarentena.

3 Se o ActiveShield não conseguir colocar o e-mail em quarentena, clique em **Excluir os anexos infectados** para tentar remover o arquivo.

Gerenciando scripts suspeitos

1 Se o ActiveShield detectar um script suspeito, você poderá obter mais informações e, em seguida, interromper o script se não tiver a intenção de iniciá-lo.

   a Clique em **Obter mais informações** para exibir o nome, o local e a descrição da atividade associada ao script suspeito.

   b Clique em **Interromper este script** para impedir que scripts suspeitos sejam executados.

2 Se você tiver certeza de que o script é confiável, poderá permitir sua execução:

   a Clique em **Permitir este script desta vez** para permitir que todos os scripts contidos em um único arquivo sejam executados de uma só vez.

   b Clique em **Continuar o que eu estava fazendo** para ignorar o alerta e permitir a execução do script.

Gerenciando possíveis worms

1 Se o ActiveShield detectar um possível worm, você poderá obter mais informações e, em seguida, interromper a atividade de e-mail se não tiver a intenção de iniciá-lo:

   a Clique em **Obter mais informações** para exibir a lista de destinatários, a linha de assunto, o corpo da mensagem e a descrição da atividade suspeita associada à mensagem de e-mail infectada.

   b Clique em **Interromper este e-mail** para impedir que o e-mail suspeito seja enviado e excluído da fila de mensagens.

2 Se você tiver certeza de que a atividade de e-mail é confiável, clique em **Continuar o que eu estava fazendo** para ignorar o alerta e permitir o envio do e-mail.

Fazendo a varredura manual do computador

O recurso Fazer varredura permite que você procure vírus e programas potencialmente indesejados em unidades de disco rígido, disquetes, e arquivos e pastas individuais. Ao encontrar um arquivo infectado, o mecanismo tenta limpá-lo automaticamente, a não ser que seja um programa potencialmente indesejado. Se o mecanismo de varredura não conseguir limpar o vírus, você poderá colocar o arquivo em quarentena ou excluí-lo.

Fazendo a varredura manual para vírus e programas potencialmente indesejados

Para fazer a varredura do computador:

1 Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Fazer varredura**.

A caixa de diálogo **Fazer varredura** será aberta (Figura 2-7).

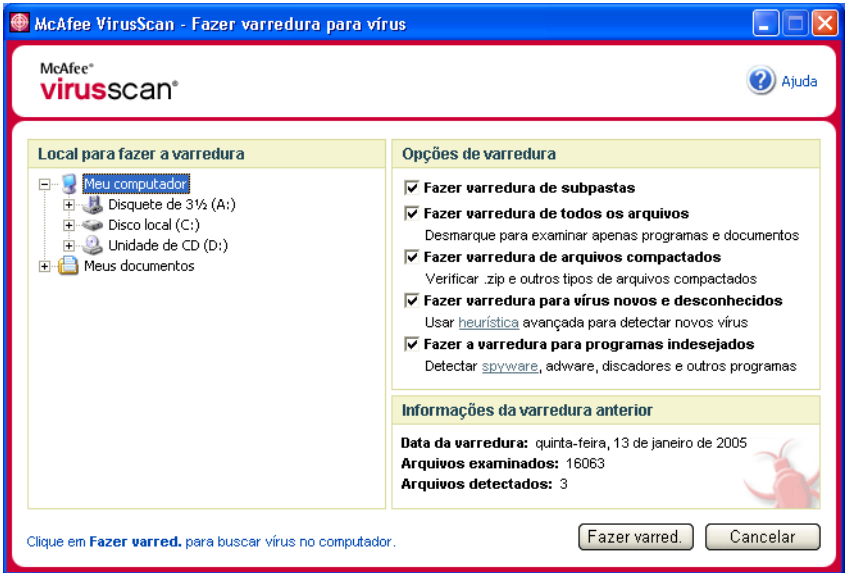

McAfee VirusScan - Fazer varredura para vírus
McAfee
virusscan
Ajuda
Local para fazer a varredura
Meu computador
Disquete de 3½ (A:)
Disco local (C:)
Unidade de CD (D:)
Meus documentos
Opções de varredura
Fazer varredura de subpastas
Fazer varredura de todos os arquivos
Desmarque para examinar apenas programas e documentos
Fazer varredura de arquivos compactados
Verificar .zip e outros tipos de arquivos compactados
Fazer varredura para vírus novos e desconhecidos
Usar heurística avançada para detectar novos vírus
Fazer a varredura para programas indesejados
Detectar spyware, adware, discadores e outros programas
Informações da varredura anterior
Data da varredura: quinta-feira, 13 de janeiro de 2005
Arquivos examinados: 16063
Arquivos detectados: 3
Clique em Fazer varred. para buscar vírus no computador.
Fazer varred.
Cancelar

Figura 2-7. Fazer varredura

2 Clique na unidade, pasta ou arquivo em que será feita a varredura.

3 Selecione **Opções de varredura**. Por padrão, todas as **Opções de varredura** são previamente selecionadas para fornecer a varredura mais completa possível (Figura 2-7 na página 28):

- **Fazer varredura de subpastas** — Use esta opção para fazer a varredura dos arquivos contidos nas subpastas. Desmarque esta caixa de seleção para que a verificação seja feita somente nos arquivos visíveis quando você abre uma pasta ou unidade.

  Exemplo: Os arquivos da Figura 2-8 serão os únicos examinados se você desmarcar a caixa de seleção **Fazer varredura de subpastas**. As pastas e seu conteúdo não serão examinados. Para fazer a varredura dessas pastas e de seu conteúdo, deixe a caixa de seleção marcada.

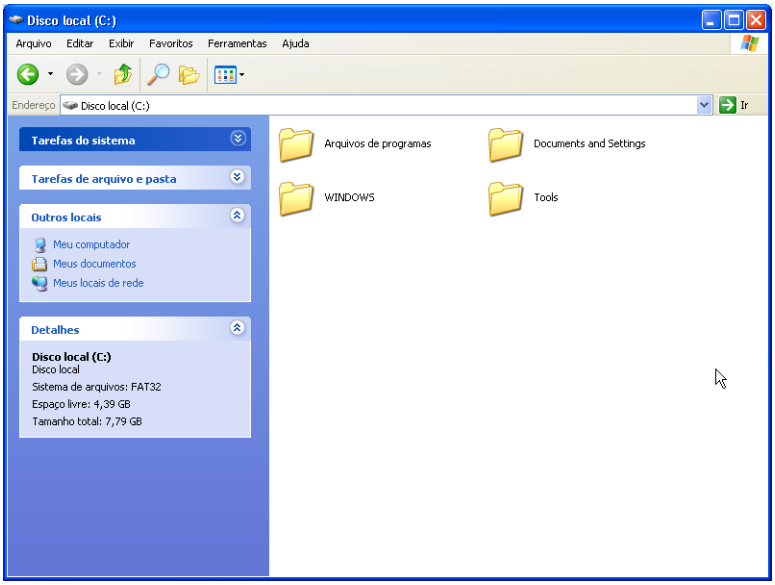


Figura 2-8. Conteúdo do disco local

- **Fazer varredura de todos os arquivos** — Use esta opção para permitir a varredura completa de todos os tipos de arquivo. Desmarque esta caixa de seleção para diminuir o tempo de varredura e permitir a verificação somente de arquivos de programa e documentos.

- **Fazer varredura de arquivos compactados** — Use esta opção para exibir arquivos infectados ocultos em arquivos .ZIP e outros arquivos compactados. Desmarque esta caixa de seleção para impedir a verificação de quaisquer arquivos ou de arquivos compactados dentro de outros arquivos compactados.

  Às vezes, os criadores de vírus colocam os vírus em um arquivo .ZIP e o insere em outro arquivo .ZIP para tentar burlar os mecanismos antivírus. O mecanismo de varredura pode detectar esses vírus desde que essa opção esteja selecionada.

- **Fazer varredura para vírus novos e desconhecidos** — Use esta opção para localizar os vírus mais recentes que podem não ter "remédio". Esta opção usa técnicas heurísticas avançadas que tentam fazer a correspondência dos arquivos com as assinaturas de vírus conhecidos e, ao mesmo tempo, procura indícios de vírus desconhecidos nos arquivos.

  Este método de varredura também procura características nos arquivos que geralmente indicam que ele contém vírus. Isso minimiza as chances de a varredura apresentar indicações falsas. Contudo, se uma varredura heurística detectar um vírus, você deverá tratá-lo com o mesmo cuidado que trataria um arquivo que você sabe que contém vírus.

  Esta opção fornece a varredura mais completa, mas geralmente é mais lenta do que uma varredura normal.

- **Fazer varredura para programas potencialmente indesejados** — Use esta opção para detectar spyware, adware, discadores e outros programas que você não pretende instalar em seu computador.

  OBSERVAÇÃO
  Deixe todas as opções selecionadas para obter a varredura mais completa possível. Esse procedimento fará a varredura em todos os arquivos da unidade ou pasta selecionada. Portanto, reserve tempo suficiente para que a varredura seja concluída. Quanto maior a unidade de disco rígido e o número de arquivos que ela contém, mais demorada será a varredura.

4 Clique em **Fazer varredura** para iniciar a varredura dos arquivos.

Quando a varredura for concluída, um resumo informará o número de arquivos examinados e de arquivos detectados, além do número de programas potencialmente indesejados e arquivos detectados que foram limpos automaticamente.

5 Clique em **OK** para fechar o resumo e exibir a lista dos arquivos detectados na caixa de diálogo **Fazer varredura** (Figura 2-9).

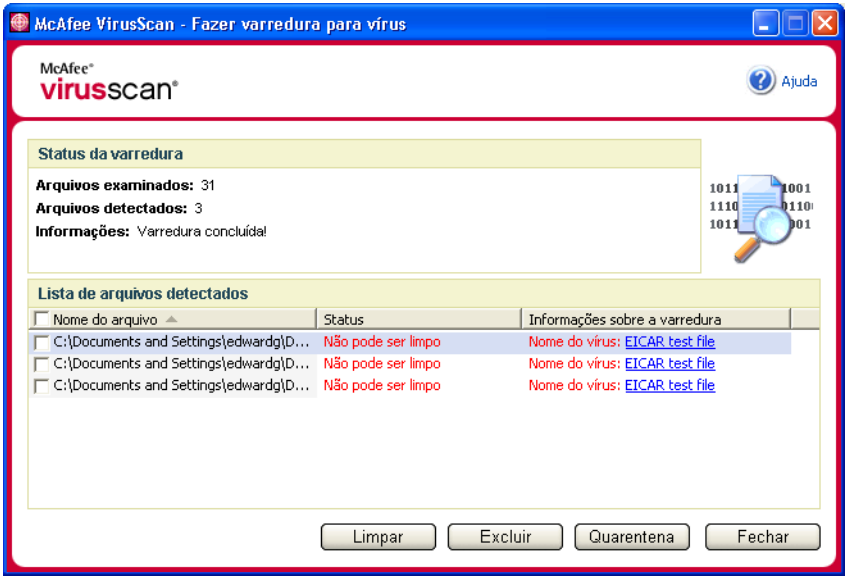


Figura 2-9. Resultados da varredura

OBSERVAÇÃO
A varredura inclui um arquivo compactado (.ZIP, .CAB etc.) na contagem dos **Arquivos examinados**. Além disso, o número de arquivos examinados pode variar se você excluiu os arquivos temporários da Internet após a última varredura.

6 Se o mecanismo de varredura não encontrar vírus ou programas potencialmente indesejados, clique em **Voltar** para selecionar outra pasta ou unidade para a varredura ou clique em **Fechar** para fechar a caixa de diálogo. Caso contrário, consulte *Se a opção Fazer varredura encontrar um vírus ou programa potencialmente indesejado* na página 35.

Fazendo a varredura pelo Windows Explorer

O VirusScan fornece um menu de atalho que permite fazer a varredura de arquivos, pastas ou unidades a partir do Windows Explorer em busca de vírus e programas potencialmente indesejados.

Para fazer a varredura de arquivos no Windows Explorer:

1. Abra o Windows Explorer.
2. Clique com o botão direito do mouse na unidade, na pasta ou no arquivo em que a varredura será feita e clique em **Fazer varredura**.

   A caixa de diálogo **Fazer varredura** será aberta e iniciará a varredura dos arquivos. Por padrão, todas as **Opções de varredura** padrão são previamente selecionadas para fornecer a varredura mais completa possível (Figura 2-7 na página 28).

Fazendo a varredura pelo Microsoft Outlook

O VirusScan possui um ícone de barra de ferramentas para o Microsoft Outlook 97 ou posterior que permite verificar se há vírus ou programas potencialmente indesejados nos armazenamentos de mensagem selecionados e respectivas subpastas, pastas de caixa de correio ou mensagens de e-mail com anexos.

Para fazer a varredura de e-mails no Microsoft Outlook:

1. Abra o Microsoft Outlook.
2. Clique no armazenamento de mensagem, pasta ou mensagem de e-mail que contém um anexo a ser examinado e, em seguida, clique no ícone da barra de ferramentas de varredura de e-mail .

   O mecanismo de varredura de e-mail é aberto e inicia a varredura dos arquivos. Por padrão, todas as **Opções de varredura** padrão são previamente selecionadas para fornecer a varredura mais completa possível (Figura 2-7 na página 28).

Fazendo a varredura automática para vírus e programas potencialmente indesejados

Embora o VirusScan faça a varredura de arquivos à medida que são acessados por você ou por seu computador, é possível programar a varredura automática no Agendador do Windows para procurar minuciosamente vírus e programas potencialmente indesejados no computador em intervalos especificados.

Para programar uma varredura:

1 Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Opções**.

A caixa de diálogo **Opções do VirusScan** será aberta.

2 Clique na guia **Varredura programada** (Figura 2-10).

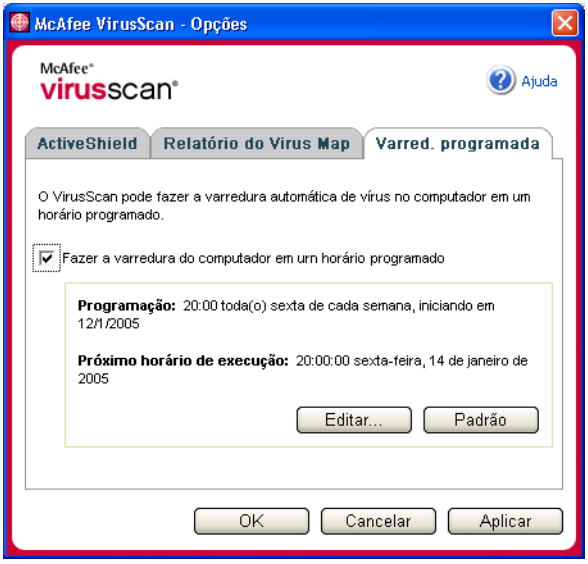

McAfee VirusScan - Opções
McAfee
virusscan
Ajuda
ActiveShield
Relatório do Vírus Map
Varred. programada
O VirusScan pode fazer a varredura automática de vírus no computador em um horário programado.
Fazer a varredura do computador em um horário programado
Programação: 20:00 toda(o) sexta de cada semana, iniciando em 12/1/2005
Próximo horário de execução: 20:00:00 sexta-feira, 14 de janeiro de 2005
Editar...
Padrão
OK
Cancelar
Aplicar

Figura 2-10. Opções de Varredura programada

3 Marque a caixa de seleção **Fazer a varredura do computador em um horário programado** para ativar a varredura automática.

4 Especifique uma programação para a varredura automática:

- Para aceitar a programação padrão (Todas as sextas-feiras às 20:00 h), clique em **OK**.
- Para editar a programação:

  a. Clique em **Editar**.

  b. Na lista **Programar tarefa**, selecione a freqüência em que o computador será submetido a uma varredura e, em seguida, selecione opções adicionais na área dinâmica abaixo dela:

  Diariamente — Especifique o número de dias entre as varreduras.

  Semanalmente (padrão) — Especifique o número de semanas entre as varreduras, bem como o(s) dia(s) da semana.

  Mensalmente — Especifique em qual dia do mês será feita a varredura. Clique em **Selecionar meses** para especificar em quais meses a varredura será feita e, depois, clique em **OK**.

  Uma vez — Especifique em qual data a varredura será feita.

  OBSERVAÇÃO
  Estas opções do Agendador do Windows não são suportadas: **Ao inicializar o sistema**, **Quando ocioso** e **Mostrar vários agendamentos**. A última programação com suporte permanecerá ativada até você selecionar uma das opções válidas.

  c. Na caixa **Hora de início**, selecione a hora do dia em que a varredura do computador será feita.

  d. Para selecionar opções avançadas, clique em **Avançado**.

  A caixa de diálogo **Opções de programação avançadas** será aberta.

  i. Especifique uma data de início, data de término, duração, hora de término e se deseja interromper a tarefa em um horário específico caso a varredura ainda esteja sendo executada.

  ii. Clique em **OK** para salvar as alterações e fechar a caixa de diálogo. Caso contrário, clique em **Cancelar**.

5 Clique em **OK** para salvar as alterações e fechar a caixa de diálogo. Caso contrário, clique em **Cancelar**.

6 Para retornar à programação padrão, clique em **Padrão**. Caso contrário, clique em **OK**.

Se a opção Fazer varredura encontrar um vírus ou programa potencialmente indesejado

Para a maioria dos vírus, Cavalos de Tróia e worms, a opção Fazer varredura tenta limpar automaticamente o arquivo. Em seguida, você pode especificar como gerenciará os arquivos infectados, inclusive se deseja enviá-los aos laboratórios AVERT da McAfee para serem pesquisados. Se a opção Fazer varredura detectar um programa potencialmente indesejado, tente limpá-lo manualmente, colocá-lo em quarentena ou excluí-lo (o envio para a AVERT não está disponível).

Para gerenciar um vírus ou programa potencialmente indesejado:

1. Se um arquivo for exibido na **Lista de arquivos detectados**, clique na caixa de seleção que aparece na frente do arquivo para selecioná-lo.

   OBSERVAÇÃO
   Se mais de um arquivo for exibido na lista, você poderá marcar a caixa de seleção exibida na frente da lista **Nome do arquivo** para executar a mesma ação em todos os arquivos. Você também pode clicar no nome do arquivo na lista **Informações sobre a varredura** para exibir os detalhes da Biblioteca de informações sobre vírus.

2. Se o arquivo for um programa potencialmente indesejado, clique em **Limpar** para tentar limpá-lo.

3. Se a opção Fazer varredura não conseguir limpar o arquivo, clique em **Quarentena** para criptografar e isolar temporariamente arquivos infectados e suspeitos no diretório de quarentena até que uma ação apropriada possa ser executada. (Consulte *Gerenciando arquivos em quarentena* para obter detalhes.)

4. Se o mecanismo de varredura não conseguir limpar o arquivo ou colocá-lo em quarentena, você poderá executar uma destas ações:

   - Clique em **Excluir** para remover o arquivo.
   - Clique em **Cancelar** para fechar a caixa de diálogo sem que seja necessário nenhuma outra ação.

Se a opção Fazer varredura não conseguir limpar ou excluir o arquivo detectado, consulte Biblioteca de informações sobre vírus em http://br.mcafee.com/virusInfo/default.asp para obter instruções sobre como excluir o vírus manualmente.

Se um arquivo detectado não permitir que você use a conexão com a Internet ou o computador, tente usar um Disco de resgate para iniciar o computador. O Disco de resgate, em muitos casos, poderá iniciar um computador se um arquivo detectado desativá-lo. Consulte “Criando um disco de resgate” na Ajuda on-line para obter detalhes.

Para obter mais ajuda, consulte o Suporte ao cliente da McAfee em http://www.mcafeeajuda.com.

Gerenciando arquivos em quarentena

O recurso Quarentena criptografa e isola temporariamente arquivos infectados e suspeitos no diretório de quarentena até que uma ação apropriada possa ser executada. Depois de limpo, um arquivo em quarentena pode ser restaurado para o local original.

Para gerenciar um arquivo em quarentena:

1 Clique com o botão direito do mouse no ícone da McAfee, aponte para **VirusScan** e clique em **Gerenciar arquivos em quarentena**.

Uma lista de arquivos em quarenta é exibida (Figura 2-11).

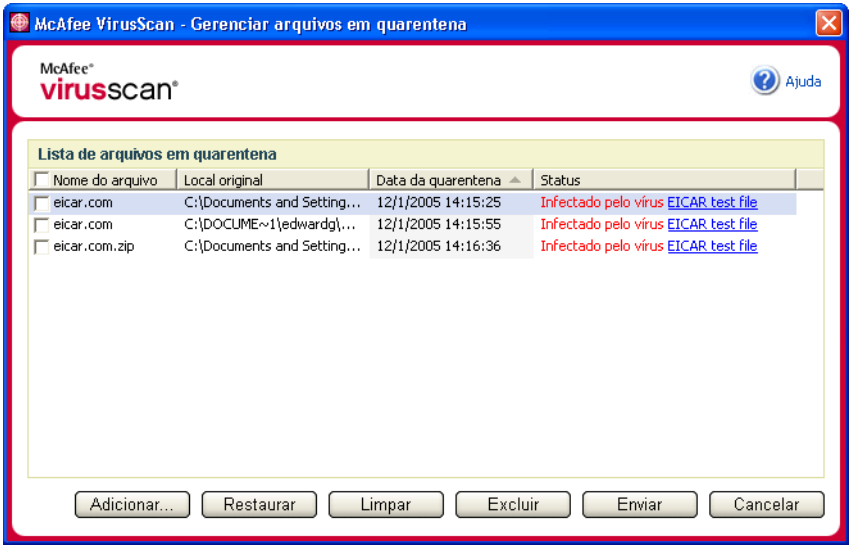


Figura 2-11. Gerenciar arquivos em quarentena

2 Marque a(s) caixa(s) de seleção próxima(s) ao(s) arquivo(s) que você deseja limpar.

> **OBSERVAÇÃO**
> Se mais de um arquivo for exibido na lista, você poderá marcar a caixa de seleção exibida na frente da lista **Nome do arquivo** para executar a mesma ação em todos os arquivos. Você também pode clicar no nome do vírus na lista **Status** para exibir os detalhes da Biblioteca de informações sobre vírus.
>
> Uma outra alternativa é clicar em **Adicionar**, selecionar um arquivo suspeito para adicionar à lista de quarentena, clicar em **Abrir** e selecioná-lo na lista de quarentena.

3 Clique em **Limpar**.

4 Se o arquivo estiver limpo, clique em **Restaurar** para devolvê-lo para o local original.

5 Se o VirusScan não conseguir limpar o vírus, clique em **Excluir** para remover o arquivo.

6 Se o VirusScan não conseguir limpar ou excluir o arquivo e se ele não for um programa potencialmente indesejado, você poderá enviá-lo à McAfee AntiVirus Emergency Response Team (AVERT™) para que seja pesquisado:

   a Atualize os arquivos de assinatura de vírus se eles tiverem mais de duas semanas.

   b Verifique a sua assinatura.

   c Selecione o arquivo e clique em **Enviar** para enviar o arquivo à AVERT.

   O VirusScan envia o arquivo em quarentena como um anexo em uma mensagem de e-mail contendo o endereço de e-mail, o país, a versão de software, o sistema operacional, além do nome e local originais do arquivo. O tamanho de envio máximo é um único arquivo de 1,5 MB por dia.

7 Clique em **Cancelar** para fechar a caixa de diálogo sem que seja necessário nenhuma outra ação.

Usando o software Professional Edition 3

O McAfee VirusScan Professional Edition contém o McAfee VirusScan, o McAfee SpamKiller e o McAfee Shredder.

OBSERVAÇÃO
Esta é apenas uma visão geral. Para obter informações detalhadas, consulte a Ajuda on-line do VirusScan, SpamKiller ou Shredder.

Usando o McAfee SpamKiller

O software McAfee SpamKiller ajuda a impedir que spams entrem em sua caixa de entrada de e-mails.

OBSERVAÇÃO
O McAfee SpamKiller filtra o MSN/Hotmail, mas atualmente não filtra as contas de e-mail do AOL, Yahoo ou outras contas com base na Internet.

Visão geral

Durante a instalação, você configurou uma ou mais contas de e-mail para as quais deseja bloquear mensagens indesejadas. Você também importou listas de endereços de e-mail para a sua lista de amigos para impedir que as mensagens de remetentes conhecidos também sejam bloqueadas.

Para gerenciar spam:

1. Abra o seu programa de e-mail para exibir, enviar e receber mensagens de e-mail, como de costume.
2. Abra o SpamKiller:

   Clique com o botão direito no ícone da McAfee , aponte para **SpamKiller** e, em seguida, clique em **Exibir e-mails bloqueados**, **Exibir resumo**, **Exibir lista de amigos** ou **Configurações**. A página correspondente é exibida:

   OBSERVAÇÃO
   Se a caixa de diálogo **Logon** for exibida, digite a sua senha de logon no SpamKiller e clique em **OK**.

Página Resumo

Clique na guia **Resumo** para abrir a página Resumo, a qual fornece as seguintes informações:

- **Status** informa se a filtragem está ativada, quando uma lista de amigos foi atualizada pela última vez e o número de mensagens de spam recebidas hoje. Nesse local, você pode desativar ou ativar a filtragem do SpamKiller, atualizar listas de amigos e abrir a página E-mail bloqueado.
- **Spam recente** mostra as mensagens de spam mais recentes bloqueadas pelo SpamKiller (mensagens removidas da caixa de entrada). Para colocar uma mensagem novamente na caixa de entrada, clique no ícone **Recuperar** ao lado da mensagem.
- **Visão geral do e-mail** exibe o número total de e-mails, spams (mensagens bloqueadas) e a porcentagem do total de spams recebidos.
- **Spam recente** fornece uma análise do tipo de spam recebido nos últimos 30 dias.

Integração entre Microsoft Outlook e Outlook Express

Você pode acessar os principais recursos do SpamKiller diretamente no Outlook Express 6.0, Outlook 98, Outlook 2000 e Outlook XP. Você pode bloquear spams, adicionar pessoas à sua lista de amigos e exibir e-mails em quarentena clicando nos botões diretamente integrados à barra de ferramentas do Outlook e Outlook Express.

- Clique no ícone **Bloquear mensagem** para remover a mensagem selecionada da caixa de entrada do Microsoft Outlook e colocá-la na pasta E-mail bloqueado do SpamKiller.
- Clique no ícone **Exibir mensagens bloqueadas** para exibir as mensagens que foram bloqueadas na conta do Microsoft Outlook e movidas para a pasta E-mail bloqueado do SpamKiller.
- Clique no ícone **Adicionar amigo** para adicionar o endereço de e-mail do remetente à Lista de amigos pessoais.

A barra de ferramentas do SpamKiller será exibida à direita das barras de ferramentas padrão do Outlook e Outlook Express. Se ela não estiver visível, expanda a janela do aplicativo de e-mail ou clique nas setas para exibir mais barras de ferramentas.

Quando a barra de ferramentas do SpamKiller for exibida pela primeira vez no aplicativo de e-mail, você poderá usar os comandos da barra de ferramentas somente em mensagens novas. Os e-mails de spam existentes devem ser excluídos.

Trabalhando com mensagens bloqueadas e aceitas

Clique na guia **Mensagens** para acessar as mensagens bloqueadas e aceitas. As páginas E-mail bloqueado e E-mail aceito possuem recursos similares.

Página E-mail bloqueado

Clique na guia **E-mail bloqueado** na página Mensagens para exibir as mensagens bloqueadas.

> **OBSERVAÇÃO**
> Você também pode acessar as mensagens bloqueadas na conta do Microsoft Outlook abrindo a caixa de entrada do Outlook e clicando em na barra de ferramentas do Microsoft Outlook ou Outlook Express.

As mensagens bloqueadas são aquelas que o SpamKiller identificou como spam, removeu da caixa de entrada e colocou na pasta E-mail bloqueado.

A página E-mail bloqueado exibe todas as mensagens de spam removidas das contas de e-mail. Para exibir os e-mails bloqueados de uma conta específica, clique na seta para baixo localizada na guia **E-mail bloqueado** e selecione a conta a ser exibida.

O painel de mensagens superior lista as mensagens de spam classificadas por data. A mensagem mais recente é exibida primeiro. O painel de visualização inferior contém o texto da mensagem selecionada.

> **OBSERVAÇÃO**
> Se o computador estiver executando o Windows 2000 ou Windows XP, vários usuários tiverem sido adicionados ao SpamKiller e você estiver conectado ao SpamKiller como usuário limitado, o conteúdo da mensagem não será exibido no painel de visualização inferior.

O painel do meio exibe os detalhes da mensagem. Clique nas setas para baixo a fim de expandir o painel de detalhes da mensagem, e exibir o texto da mensagem e os cabeçalhos no formato nativo, incluindo quaisquer guias de formatação HTML. O painel de detalhes da mensagem mostra o seguinte:

- **Ação** descreve como o SpamKiller processou a mensagem de spam. Esta opção está associada à ação do filtro que bloqueou a mensagem.
- **Razão** explica por que o SpamKiller bloqueou a mensagem. Você pode clicar na razão para abrir o editor de filtros e exibir o filtro. O editor de filtros exibe o que o filtro procura em uma mensagem e a ação executada pelo SpamKiller contra as mensagens encontradas pelo filtro.
- **De** exibe o remetente da mensagem.
- **Data** exibe a data em que a mensagem foi enviada a você.

- **Para** exibe para quem a mensagem foi enviada.
- **Assunto** exibe o tópico que aparece na linha de assunto da mensagem.

A coluna da esquerda conterá ícones próximo às mensagens caso reclamações manuais ou mensagens de erro tenham sido enviadas:

Uma reclamação sobre a mensagem foi enviada.

Uma mensagem de erro será enviada para o endereço de resposta da mensagem de spam.

Uma reclamação e uma mensagem de erro foram enviadas.

Página E-mail aceito

Clique na guia **E-mail aceito** da página Mensagens para exibir as mensagens aceitas.

A página E-mail aceito exibe todas as mensagens da caixa de entrada em todas as contas de e-mail. Entretanto, para contas MAPI, a página E-mail aceito não contém e-mail interno. Para exibir os e-mails aceitos de uma conta específica, clique na seta para baixo da guia **E-mail aceito** e selecione uma conta a ser exibida.

> **OBSERVAÇÃO**
> O SpamKiller é projetado para aceitar e-mails legítimos. Entretanto, se os e-mails legítimos forem exibidos na lista de e-mails bloqueados, você poderá colocar as mensagens de volta na caixa de entrada (e na lista de e-mails aceitos), selecionando-as e clicando em **Recuperar esta mensagem**.

Assim como na página E-mail bloqueado, o painel de mensagens superior lista as mensagens classificadas por data. O painel de visualização inferior contém o texto da mensagem selecionada.

O painel do meio explica se a mensagem foi enviada por alguém de uma lista de amigos ou se a mensagem está de acordo com os critérios de um filtro, mas a ação do filtro foi definida para **Aceitar** ou **Marcar como possível spam**. Clique nas setas para baixo para expandir o painel de detalhes da mensagem e exibir o texto da mensagem e os cabeçalhos no formato nativo, incluindo quaisquer guias de formatação HTML.

O painel de detalhes da mensagem mostra o seguinte:

- **Ação** descreve como o SpamKiller processou a mensagem.
- **Razão** explica por que o SpamKiller sinalizou a mensagem.
- **De** exibe o remetente da mensagem.
- **Data** exibe a data em que a mensagem foi enviada a você.
- **Para** exibe para quem a mensagem foi enviada.
- **Assunto** exibe o tópico que aparece na linha de assunto da mensagem.

Um destes ícones é exibido próximo a uma mensagem aceita:

O SpamKiller detectou que o remetente da mensagem pertence a uma lista de amigos.

A mensagem corresponde a um filtro com uma ação definida para **Marcar como possível spam**.

Uma reclamação sobre a mensagem foi enviada.

Uma mensagem de erro será enviada para o endereço de resposta da mensagem de spam.

Uma reclamação e uma mensagem de erro foram enviadas.

Tarefas de E-mail bloqueado e E-mail aceito

O painel à direita nas páginas E-mail bloqueado e E-mail aceito lista as tarefas que você pode executar:

- **Bloquear esta mensagem** remove uma mensagem da caixa de entrada e a coloca na pasta de e-mails bloqueados do SpamKiller. (Esta opção é exibida somente na página E-mail aceito.)
- **Recuperar esta mensagem** coloca a mensagem de volta na caixa de entrada e abre a caixa de diálogo Opções de resgate. (Esta opção é exibida somente na página E-mail bloqueado.) Você pode adicionar automaticamente o remetente à lista de amigos e recuperar todas as mensagens do remetente.
- **Excluir esta mensagem** remove uma mensagem selecionada.
- **Adicionar um amigo** adiciona o nome, o endereço de e-mail, o domínio ou a lista de mala direta do remetente a uma lista de amigos.
- **Adicionar um filtro** cria um filtro.
- **Relatar à McAfee** informa a McAfee sobre as mensagens de spam que você recebeu.
- **Enviar uma reclamação** envia uma reclamação sobre spams ao administrador do domínio do remetente ou a outro endereço de e-mail que você digitar.
- **Enviar um erro** envia uma mensagem de erro para o endereço de resposta de uma mensagem de spam.

Recuperando mensagens

Se a página E-mail bloqueado contiver e-mails legítimos, você poderá colocar essas mensagens de volta na caixa de entrada.

Para recuperar uma mensagem:

1. Exiba as suas mensagens de e-mail bloqueadas:
   - No SpamKiller, clique na guia **Mensagens** e, em seguida, clique na guia **E-mail bloqueado**.
   - Na caixa de entrada do Microsoft Outlook ou Outlook Express, clique em para abrir a página E-mail bloqueado dessa conta.

   A página E-mail bloqueado será exibida.
2. Selecione uma mensagem e, em seguida, clique em **Recuperar esta mensagem**.

   A caixa de diálogo Opções de resgate é exibida com as seguintes opções padrão selecionadas:
   - **Adicionar amigo**
   - **Recuperar todas do mesmo remetente**
3. Clique em **OK**. O remetente será adicionado à sua lista de amigos, e todas as mensagens deste remetente são devolvidas à caixa de entrada e à pasta E-mail aceito.

Bloqueando mensagens

Bloqueie as mensagens de spam que estão na caixa de entrada. Quando você bloqueia uma mensagem, o SpamKiller cria automaticamente um filtro para removê-la da caixa de entrada. Você pode bloquear mensagens da caixa de entrada na página E-mail aceito, ou no Microsoft Outlook ou Outlook Express.

Para bloquear uma mensagem na página E-mail aceito:

1. Clique na guia **Mensagens** e, em seguida, clique na guia **E-mail aceito**. A página E-mail aceito será exibida com mensagens da caixa de entrada.
2. Selecione uma mensagem e, em seguida, clique em **Bloquear esta mensagem**. A mensagem é removida da caixa de entrada e da página E-mail aceito, e uma cópia da mensagem é exibida na pasta E-mail bloqueado.

Para bloquear uma mensagem no Microsoft Outlook:

1. Abra a caixa de entrada do Microsoft Outlook ou Outlook Express. Você só pode bloquear mensagens externas (mensagens vindas de um servidor da Internet).
2. Selecione uma mensagem e, em seguida, clique em . Uma cópia da mensagem é colocada na pasta E-mail bloqueado.

Excluindo mensagens

Por padrão, quando o SpamKiller encontra um spam, ele o remove da caixa de entrada e o coloca na pasta E-mail bloqueado do SpamKiller. O SpamKiller remove automaticamente as mensagens bloqueadas da pasta E-mail bloqueado após 15 dias. Você pode alterar a freqüência na qual o SpamKiller remove automaticamente as mensagens bloqueadas. Você também pode remover as mensagens manualmente.

O SpamKiller não remove automaticamente as mensagens da pasta E-mail aceito, pois ela reflete as mensagens que estão na caixa de entrada no momento.

Em vez de mover as mensagens de spam para a pasta E-mail bloqueado, o SpamKiller pode identificar a linha de assunto do e-mail com "[spam]" ou com uma marca de sua preferência, e mantê-la na caixa de entrada. A marcação de mensagens pode ser útil se você desejar mover as mensagens marcadas para outra pasta do cliente de e-mail, como uma pasta "inútil". Você pode mover as mensagens marcadas criando uma regra no cliente de e-mail, de modo que ele procure mensagens com a marca "[spam]" e as coloque na pasta que você indicar.

Para alterar a configuração da remoção automática de mensagens bloqueadas:

1. Clique na guia **Configurações** e, em seguida, no ícone **Opções de filtragem**.
2. Especifique como o SpamKiller deve tratar as mensagens de spam:
   - **Colocar o spam na caixa de e-mail bloqueado** — As mensagens de spam são removidas da caixa de entrada e colocadas na pasta E-mail bloqueado do SpamKiller.
   - **Manter o e-mail bloqueado por ____ dias** — As mensagens bloqueadas permanecem na pasta E-mail bloqueado durante o período de dias que você especificar.
   - **Marcar o spam e manter na caixa de entrada** — As mensagens de spam permanecerão na caixa de entrada, mas a linha de assunto da mensagem conterá "[spam]" ou a marca que você inserir.
3. Clique em **OK**.

Para excluir uma mensagem manualmente:

1. Exiba as suas mensagens de e-mail bloqueadas:
   - No SpamKiller, clique na guia **Mensagens** e, em seguida, clique na guia **E-mail bloqueado**.
   - Na caixa de entrada do Microsoft Outlook ou Outlook Express, clique em para abrir a página E-mail bloqueado dessa conta.

   A página E-mail bloqueado será exibida.

2 Selecione uma mensagem e, em seguida, clique em **Excluir esta mensagem**. Uma caixa de diálogo de confirmação será exibida.

3 Clique em **Sim** para excluir a mensagem.

Relatando spams à McAfee

Você pode relatar spams à McAfee para que a análise seja usada na criação de atualizações de filtros.

Para relatar spams à McAfee:

1 Clique na guia **Mensagens** e, em seguida, clique na guia **E-mail bloqueado** ou **E-mail aceito**. A página E-mail bloqueado ou E-mail aceito será exibida.

2 Selecione uma mensagem e clique em **Relatar à McAfee**. Uma caixa de diálogo de confirmação será exibida.

3 Clique em **Sim** para enviar a mensagem automaticamente à McAfee.

Enviando reclamações manualmente

Envie uma reclamação para impedir que um remetente envie mais spams para você. Consulte "Enviando reclamações e mensagens de erro" na Ajuda on-line para obter detalhes.

Para enviar uma reclamação manualmente:

1 Clique na guia **Mensagens** e, em seguida, clique na guia **E-mail bloqueado** ou **E-mail aceito**. Uma lista de mensagens será exibida.

2 Selecione uma mensagem sobre a qual fará uma reclamação e clique em **Enviar uma reclamação**. A caixa de diálogo Enviar reclamação será exibida.

3 Selecione para quem você deseja enviar a mensagem.

> **AVISO**
> Na maioria dos casos, você não deve selecionar **Remetente**. O envio de uma reclamação ao remetente do spam valida seu endereço de e-mail, o que pode aumentar o número de spams que esse remetente enviará a você.

4 Clique em **Avançar** e, em seguida, siga as instruções das caixas de diálogo exibidas.

Enviando mensagens de erro

Envie uma mensagem de erro para evitar que um remetente envie mais spams a você. Consulte "Enviando reclamações e mensagens de erro" na Ajuda on-line para obter detalhes.

Para enviar uma mensagem de erro manualmente:

1. Clique na guia **Mensagens** e, em seguida, clique na guia **E-mail bloqueado** ou **E-mail aceito**. Uma lista de mensagens será exibida.
2. Selecione uma mensagem e, em seguida, clique em **Enviar erro**. Uma mensagem de erro será enviada para o endereço de resposta da mensagem de spam.

Usando o McAfee Shredder

O McAfee Shredder protege sua privacidade eliminando, com segurança e rapidez, arquivos indesejados.

Os arquivos excluídos podem ser recuperados em seu computador até mesmo depois do esvaziamento da Lixeira. Quando você exclui um arquivo, o Windows simplesmente marca esse espaço na unidade de disco para indicar que ele não está sendo mais utilizado, mas o arquivo continua presente.

Por que o Windows deixa alguns vestígios do arquivo?

Para excluir um arquivo permanentemente, é preciso sobrescrever várias vezes o arquivo existente com novos dados. Se o Microsoft Windows excluísse os arquivos com segurança, cada operação de arquivo seria muito lenta. A destruição de um documento nem sempre impede que o documento seja recuperado, pois alguns programas fazem cópias ocultas temporárias de documentos abertos. Se você destruiu apenas os documentos exibidos no Explorer, pode ser que ainda tenha cópias temporárias desses documentos. Recomendamos que você destrua periodicamente o espaço livre na unidade de disco para garantir que as cópias temporárias sejam excluídas permanentemente.

OBSERVAÇÃO
Com ferramentas legais de computador, registros de impostos, currículos ou outros documentos excluídos podem ser recuperados.

O que o McAfee Shredder apaga?

Com o McAfee Shredder, você pode apagar permanentemente e com segurança:

- Um ou mais arquivos ou pastas
- Um disco inteiro
- Os rastros deixados pela navegação na Web

Apagando arquivos permanentemente no Windows Explorer

Para destruir um arquivo através do Windows Explorer:

1. Abra o Windows Explorer e selecione o(s) arquivo(s) a ser(em) destruído(s).
2. Clique com o botão direito do mouse no item selecionado, aponte para **Enviar para** e selecione **McAfee Shredder**.

Esvaziando a Lixeira do Windows

Se os arquivos estiverem na Lixeira, o McAfee Shredder oferecerá um método mais seguro para esvaziá-la.

Para destruir o conteúdo da Lixeira:

1. Na área de trabalho do Windows, clique com o botão direito do mouse na Lixeira.
2. Selecione **Destruir a Lixeira** e siga as instruções na tela.

Personalizando as configurações do Shredder

Você pode personalizar as configurações do Shredder:

- Especificar o número de destruições.
- Mostrar uma mensagem de aviso ao destruir arquivos.
- Verificar se há erros no disco rígido antes de destruir.
- Adicionar o McAfee Shredder ao menu Enviar para.
- Colocar um ícone do Shredder na área de trabalho do Windows.

Para personalizar as configurações do Shredder, abra o McAfee Shredder, clique em **Propriedades** e siga as instruções na tela.

Índice

A

ActiveShield
- ativando, 15
- configuração de varredura padrão, 17 a 18, 21 a 24
- desativando, 16
- fazendo a varredura de anexos de mensagens instantâneas recebidas, 21
- fazendo a varredura de e-mails e anexos, 18
- fazendo a varredura de todos os arquivos, 21
- fazendo a varredura de todos os tipos de arquivo, 21
- fazendo a varredura para scripts e worms, 23
- fazendo a varredura para vírus novos e desconhecidos, 22
- fazendo a varredura somente de arquivos de programa e documentos, 22
- iniciando, 17
- interrompendo, 17
- limpando um vírus, 25
- opções de varredura, 16
- testando, 11

alertas
- de arquivos infectados, 26
- de e-mails infectados, 26
- de possíveis worms, 27
- de scripts suspeitos, 27
- de vírus, 25

anexos de mensagens instantâneas recebidas
- fazendo a varredura, 21
- limpeza automática, 21

Assistente de atualização, 17

AVERT, enviando arquivos suspeitos a, 37

C

Cavalos de Tróia
- alertas, 25
- detectando, 35

configurando
- VirusScan
  - ActiveShield, 15
  - Fazer varredura, 28

D

Disco de resgate, 35

E

e-mails e anexos
- colocando em quarentena, 26
- desativando a limpeza automática, 20
- excluindo, 26
- fazendo a varredura, 18
- limpando, 26
- limpeza automática, 18

enviando arquivos suspeitos à AVERT, 37

F

fazendo a varredura
- arquivos compactados, 30
- de subpastas, 29
- para scripts e worms, 23
- para vírus novos e desconhecidos, 30
- pela barra de ferramentas do Microsoft Outlook, 32
- pelo Windows Explorer, 32
- programando varreduras automáticas, 33
- somente arquivos de programa e documentos, 22
- todos os arquivos, 21, 29

Fazer varredura
- colocando um vírus ou programa potencialmente indesejado em quarentena, 35
- excluindo um vírus ou programa potencialmente indesejado, 35
- fazendo a varredura manual pela barra de ferramentas do Microsoft Outlook, 32

fazendo a varredura manual pelo Windows Explorer, 32
fazer a varredura para programas potencialmente indesejados, 30
limpando um vírus ou programa potencialmente indesejado, 35
opção Fazer varredura de arquivos compactados, 30
opção Fazer varredura de subpastas, 29
opção Fazer varredura de todos os arquivos, 29
opção Fazer varredura para vírus novos e desconhecidos, 30
testando, 12 a 13
varredura automática, 33
varredura manual, 28

I

introdução ao VirusScan, 9

L

lista de arquivos detectados (Fazer varredura), 31, 35

M

McAfee SecurityCenter, 14
Microsoft Outlook, 32

N

novos recursos, 9

O

opção Fazer varredura de arquivos compactados (Fazer varredura), 30
opção Fazer varredura de subpastas (Fazer varredura), 29
opção Fazer varredura de todos os arquivos (Fazer varredura), 29
opção Fazer varredura para programas potencialmente indesejados (Fazer varredura), 30
opção Fazer varredura para vírus novos e desconhecidos (Fazer varredura), 30
opções de varredura
ActiveShield, 16, 21 a 22
Fazer varredura, 28

P

página E-mail aceito
bloqueando mensagens, 44
tarefas, 43
visão geral, 42
página E-mail bloqueado
enviando mensagens de erro, 47
excluindo mensagens bloqueadas, 45
ícones de mensagem bloqueada, 42
recuperando mensagens, 44
tarefas, 43
visão geral, 41
programando varreduras, 33
programas potencialmente indesejados
colocando em quarentena, 35
detectando, 35
excluindo, 35
limpando, 35

Q

Quarentena
adicionando arquivos suspeitos, 36
enviando arquivos suspeitos, 37
excluindo arquivos, 36
excluindo arquivos suspeitos, 37
gerenciando arquivos suspeitos, 36
limpando arquivos, 36 a 37
restaurando arquivos limpos, 36 a 37
Quick Start Card, iii

R

requisitos do sistema, 11

S

scripts
alertas, 27
interrompendo, 27
permitindo, 27
ScriptStopper, 23
Shredder
Apagando arquivos no Windows Explorer, 48
esvaziando a Lixeira do Windows, 49
opções, 49

tipos de arquivos apagados, 48
Vestígios de arquivos do Windows, 48
visão geral, 48
SpamKiller, 39
bloqueando mensagens, 44
enviando mensagens de erro, 47
enviando reclamações manualmente, 46
excluindo mensagens bloqueadas, 45
ícones de mensagem bloqueada, 42
página E-mail aceito, 42
página E-mail bloqueado, 41
recuperando mensagens, 44
relatando spams à McAfee, 46
suporte técnico, 35

T

testando o VirusScan, 11

V

vírus
alertas, 25
colocando arquivos infectados em quarentena, 26
colocando em quarentena, 25, 35
colocando em quarentena anexos de e-mail infectados, 26
detectando, 35
detectando com o ActiveShield, 25
excluindo, 25, 35
excluindo anexos de e-mail infectados, 26
excluindo arquivos infectados, 26
interrompendo possíveis vírus, 27
interrompendo scripts suspeitos, 27
limpando, 25, 35
limpando anexos de e-mail infectados, 26
permitindo scripts suspeitos, 27
VirusScan
fazendo a varredura pela barra de ferramentas do Microsoft Outlook, 32
fazendo a varredura pelo Windows Explorer, 32
introdução, 9
programando varreduras, 33
testando, 11

W

Windows Explorer, 32
worms
alertas, 25, 27
detectando, 25, 35
interrompendo, 27
WormStopper, 23

Para obter mais informações sobre produtos,
serviços mundiais e suporte, entre em contato
com seu representante de vendas autorizado da
McAfee do Brasil
R. Verbo Divino, 1227 2o. Andar
Chácara Sto Antonio São Paulo - SP 04719-002
Brasil
ou ligue para:
(55 11) 5180 6610
(55 11) 5180 6686 fax
br.mcafee.com
http://www.mcafeeajuda.com

NA-675-0010-B-1